IT-УГРОЗА С ЧЕЛОВЕЧЕСКИМ ЛИЦОМ

КАК СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ ОТКРЫВАЕТ ХАКЕРУ ДВЕРИ В ВАШУ ОРГАНИЗАЦИЮ

В рамках сотрудничества редакции «ВС» и компании Positive Technologies – одного из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений предлагаем вниманию читателей обзор очередного исследования по оценке осведомленности сотрудников в вопросах информационной безопасности (ИБ). В материалах представлена статистика и аналитические данные по результатам десяти наиболее показательных проектов за два минувших года. Работы основаны на использовании различных методов социальной инженерии и, как правило, связаны с рассылкой электронных писем, телефонным взаимодействием, а также общением через социальные сети.

Как притворяются «белые» хакеры

Слабым звеном в любой системе защиты по-прежнему остается человеческий фактор. Поэтому сегодня как никогда возрастает потребность в обучении сотрудников основам ИБ. Продуктивный способ научиться противостоять кибермошенникам – реальная практика, которая предполагает воспроизведение действий потенциального нарушителя без ущерба корпоративной инфраструктуре.

В ходе работ по оценке осведомленности сотрудников эксперты Positive Technologies проводят серию согласованных тестовых атак, имитирующих реальную деятельность злоумышленников, и отслеживают реакцию сотрудников на них. Специалисты отправляют письма, в которых содержится ссылка для перехода на специально созданный ресурс, где размещена форма для ввода учетных данных. Письма могут также содержать приложенный файл – как правило, это офисный документ с исполняемым вложением или некий архив.

Предварительно эксперты собирают адреса электронной почты сотрудников из открытых источников (как это обычно и делают злоумышленники), затем согласовывают полученный набор с компанией-заказчиком, которая либо удаляет лишние, либо добавляет другие электронные адреса, которые считает необходимыми. Рассылка проводится на адреса домена той организации, в отношении которой ведутся работы. Сотрудники, которым отправляются письма, разделены на фокус-группы, для каждой группы формируется отдельный сценарий. В результате мы можем корректно оценить, какой из сценариев будет успешнее при целевой атаке на организацию. В данном исследовании оценка проводилась на основе 3332 отправленных писем, содержащих ссылки на веб-ресурсы, формы для ввода паролей и приложенные файлы.

Отметим, что при рассылке использовались безвредные файлы, а в ходе эксперимента фиксировался только запуск. Для киберпреступников часто достаточно, чтобы пользователь просто скачал и запустил файл, хотя иногда требуется разрешить установку ПО или внесение изменений от имени администратора. Наши проверки показали, что в общей сложности 17 % всех писем в реальной жизни могли бы привести к компрометации компьютера сотрудника, а впоследствии и всей корпоративной инфраструктуры.

Ожидаемо наиболее успешным оказался метод социальной инженерии с применением фишинговой ссылки: 27 % сотрудников перешли по ссылке. Пользователи невнимательно читают адрес ссылки или не глядя кликают на него и переходят на поддельный ресурс. Когда же предлагается скачать файл, а затем запустить его, то с каждым дополнительным действием у них появляются подозрения. Поэтому лишь 7 % сотрудников оказались невнимательными и попались на удочку.

Схема реальной атаки может выглядеть следующим образом. Злоумышленник размещает на подконтрольном ресурсе набор эксплойтов под различные версии ПО. Ссылка на этот ресурс массово рассылается в фишинговых письмах. Сотрудник организации переходит по ссылке из письма, и после открытия страницы в браузере происходит эксплуатация уязвимостей, что может привести к заражению рабочей станции пользователя вредоносным ПО. Например, при использовании устаревшей версии браузера Internet Explorer может быть реализовано удаленное выполнение кода (CVE-2016-0189), ведущее к получению полного контроля над компьютером сотрудника. При этом он даже не заметит, что злоумышленник уже «поселился» в его компьютере. Приложенный к письму файл также может содержать сразу несколько эксплойтов, направленных на использование различных недостатков в ПО. Существует целый набор уязвимостей, которые могут быть использованы нарушителем (CVE-2017-0037, CVE-2012-0158, CVE-2017-0199 и др.).

Должности сотрудников, вступивших в переписку

Так, в ноябре 2017 г. злоумышленники рассылали документы, содержащие в качестве вредоносной нагрузки шифровальщик qkG[1]. В случае если пользователь скачивал полученный файл и разрешал выполнение макросов, то после закрытия такого документа на компьютере жертвы шифровалось содержимое всех документов, добавлялось текстовое сообщение с требованием выкупа, а шифровальщик мог распространяться дальше и вызвать эпидемию в инфраструктуре компании.

Для повышения эффективности злоумышленники часто сочетают различные способы атаки на пользователя. Фишинговое письмо может содержать одновременно вложение с набором вредоносных скриптов и ссылку на поддельный ресурс, где размещены не только связка эксплойтов, но и форма для ввода учетных данных. Даже современное и обновленное ПО, применяемое в инфраструктуре, и соответствующие антивирусные средства не спасут положение, если пользователь сам отдаст свой пароль в руки мошенников, введя его в некой форме на поддельном сайте.

Сотрудники – невольные соучастники

Если с переходом по ссылке, вводом своих учетных данных на поддельном сайте и запуском подозрительного файла все более-менее ясно, то почему же не стоит вступать в переписку со злоумышленником? Давайте посмотрим, в чем кроется опасность и кто обычно так поступает.

В 88 % случаев в переписку вступают сотрудники компании, не являющиеся IT-специалистами (бухгалтеры, юристы, менеджеры и т. п.). Каждый четвертый сотрудник при этом являлся руководителем отдела. Интересно, что среди вступивших в переписку были в т. ч. специалисты по ИБ, и, хотя они были в меньшинстве (3 %), это

[1] *blog.trendmicro.com/trendlabs-security-intelligence/qkg-filecoder-self-replicating-document-encrypting-ransomware/.*

лишний раз доказывает, что социальная инженерия – мощный инструмент в руках злоумышленников и даже самые осведомленные в вопросах ИБ сотрудники могут ошибиться.

Что же обычно пишут сотрудники, когда получают необычное письмо?

Как правило, пользователь сообщает, что ссылка или вложение не открывается, после чего в журналах регистрации событий на используемом при тестировании сервере сбора информации можно обнаружить, как этот пользователь многократно переходил по фишинговой ссылке, вводил различные вариации своего пароля, а затем еще и пароли к другим ресурсам. В отдельных случаях это повторялось 30–40 раз!

Иногда сотрудники писали нам «Вы ошиблись адресатом» и указывали, кому еще (по их мнению) следует направить данное письмо.

Чем это грозит? Как только злоумышленник убедился, что сотрудник принял его за коллегу или какое-то доверенное лицо, в ходе дальнейшей переписки он попытается получить нужную ему информацию, не вызывая подозрений. Так можно узнать версию используемого ПО, электронную почту других сотрудников, номера мобильных телефонов, выяснить, есть ли антивирус на рабочем компьютере, какова структура компании. Все это представляет ценность и может использоваться при планировании и проведении последующих социотехнических атак.

Иногда бывает, что сотрудники непреднамеренно помогают злоумышленнику в развитии атаки, пересылая зараженное письмо коллегам с просьбой открыть вложение или перейти по ссылке. В практике такое тоже случается. Например, сотрудники компании-заказчика перенаправляли полученные письма в IT-департамент, требуя разобраться, почему у них не открывается файл «График_отпусков.xls». Стоит отметить, что после этого специалисты IT-департамента открывали письмо и запускали файл уже у себя, видимо, доверяя письму, полученному от коллеги, которого знают лично.

Поскольку перечень сотрудников, в отношении которых проводятся такие работы, оговаривается и утверждается заранее, то довольно странно обнаружить, что скачивали и запускали рассылаемый файл совсем другие люди, не входящие в согласованные заранее фокус-группы. Именно так мы понимали, что сотрудники уже начали пересылать наше письмо своим коллегам самостоятельно. Таким образом, письмо могло доходить до рабочих станций системных администраторов и специалистов по безопасности, о которых нам не было известно при изначальной рассылке.

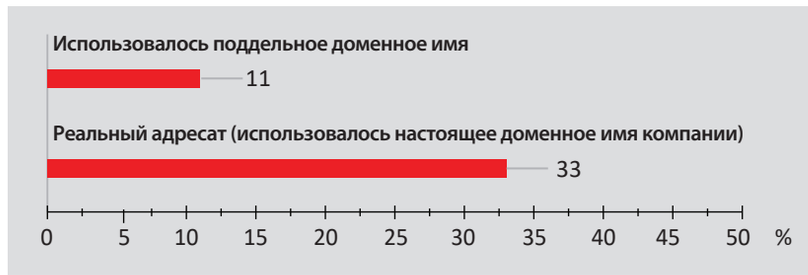
Важный момент при проведении работ по анализу защищенности – это реакция со стороны специалистов по ИБ. Что касается реагирования на фишинговые рассылки, то в тех случаях, когда работы проводились без уведомления специалистов подразделения ИБ, своевременное обнаружение подобных писем с последующей их фильтрацией и блокировкой фишингового ресурса встретилось лишь на двух проектах.

Втереться в доверие

Для проведения работ эксперты Positive Technologies регистрируют домены, которые по написанию схожи с реальными доменами компаний-заказчиков. К этому трюку часто прибегают и реальные злоумышленники: не каждый сотрудник обратит внимание, что какая-то буква в названии написана неверно либо к имени компании добавлена приставка/постфикс. При этом проверить принадлежность доменного имени компании с помощью общедоступных интернет-сервисов могут, как правило, только разбирающиеся в информационных технологиях люди. Но одно дело, если распознать подделку действительно сложно, например когда используется настоящее доменное имя организации или доверенного партнера, и совсем другое, когда письмо пришло явно с поддельного доменного имени, например admin@excamplle.com. В таких случаях речь идет о банальной невнимательности либо полном отсутствии знаний в вопросах ИБ.

В октябре 2017 г. была осуществлена фишинговая рассылка[2] от имени администрации популярного онлайн-криптокошелька MyEtherWallet. В письме было указано, что сейчас якобы проводится обновление ПО и учетные записи заблокированы, а для их разблокировки и подтверждения баланса нужно перейти по ссылке.

При переходе по ссылке открывался сайт, как две капли воды похожий на оригинальный



Результативность рассылок в зависимости от отправителя

[2] *dearbytes.com/blog/cryptocurrency-phishing/.*

myetherwallet.com. Разница была в том, что вместо последней буквы t использовался практически идентичный символ ţ в кодировке Unicode.

На какие только ухищрения не идут злоумышленники – использование Unicode, добавление дефиса к реальному имени домена, подмена похожих или созвучных букв, добавление приставок и постфиксов. Тем не менее мы считаем, что использование этой уловки неминуемо будет сходить на нет с повышением уровня осведомленности рядовых пользователей в вопросах ИБ.

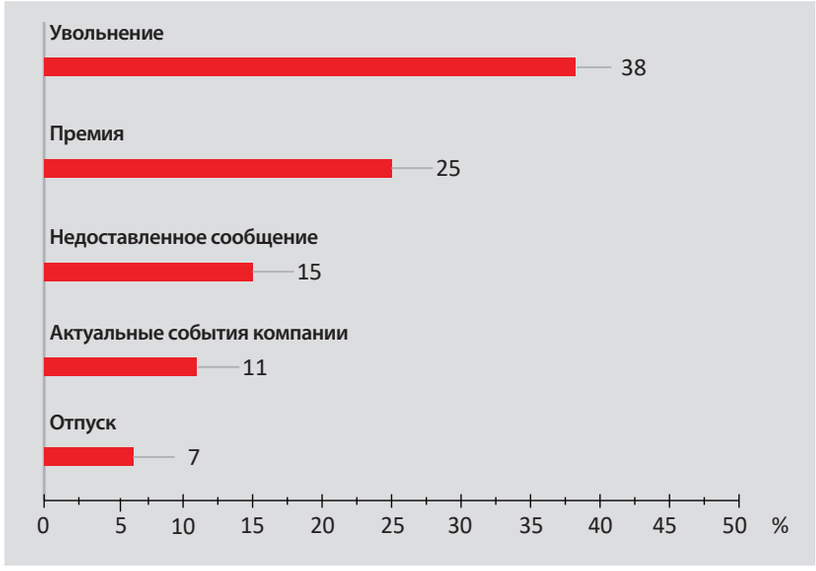
Наша практика подтверждает: 33 % пользователей совершали потенциально опасное действие, если письмо пришло от реального адресата (использовалось настоящее доменное имя какой-либо компании). В случае когда использовалось поддельное доменное имя, это происходило значительно реже: лишь 11 % сотрудников поверили собеседнику.

Вероятно, поэтому нарушители сегодня стали переходить к рассылке от имени контрагентов вместо использования поддельных доменов. Можно вспомнить группировку Cobalt[3], которая в качестве исходного вектора заражения инфраструктуры использовала фишинговые письма не только через поддельные доменные имена, но и от лица сотрудников реальных банков и компаний-интеграторов, инфраструктура которых была предварительно взломана для проведения подобных рассылок.

Тема решает все

Злоумышленники часто опираются на страх, жадность, надежды, ожидания и другие эмоции, которые могут заставить пользователя поддаться сиюминутной слабости. Когда внезапно на почту приходит письмо «Недоставленное сообщение: список сотрудников на увольнение», пользователь забывает об элементарных правилах техники кибербезопасности, он даже не задумывается, почему ему вообще пришло уведомление о недоставленном сообщении.

Часто бывает, что именно тема письма побуждает сотрудника открыть его, перейти по ссылке, скачать и запустить файл, не разбираясь, кто адресат и почему домен отправителя написан как-то странно. Если недостаточно внимательно отнестись к прочтению такого письма, то подвох заметить непросто. Самые



Темы тестовых писем (доля успешных сценариев)

эффективные сценарии фишинга, используемые в наших рассылках, приведены на диаграмме.

Предсказуемо страх увольнения или сокращения – достаточно мощный фактор, чтобы забыть о правилах ИБ: почти 40 % (!) тестовых фишинговых писем с такой темой побуждали пользователей совершить потенциально опасное действие. Высокий процент успеха показывают письма, где есть слова «премия», «поощрение», «повышение зарплаты»: каждое четвертое письмо обмануло сотрудника. Злоумышленник может также попытаться привязать тему рассылки к какому-то знаменательному событию (если располагает, например, сведениями о недавно прошедшем в компании корпоративе), профессиональным и государственным праздникам. В нашей практике 11 % писем с подобной темой стали причиной совершения потенциально опасного действия.

[3] *ptsecurity.com/upload/corporate/ru-ru/analytics/Cobalt-Snatch-rus.pdf.*

Позвони мне, позвони!

Хотя электронная почта и является наиболее распространенным и эффективным инструментом социальной инженерии, благодаря возможному охвату и простоте реализации, это далеко не единственный метод, который используют злоумышленники. Они могут позвонить по телефону, представляясь специалистом технической поддержки, и попытаться получить критически важные данные или обманом заставить сотрудника перейти по нужной ссылке, ввести пароль, скачать и запустить посторонний файл. Классический пример – звонок рано утром в воскресенье с просьбой срочно явиться на работу. Затем в ходе разговора выясняется, что можно просто предоставить свой пароль от компьютера, и тогда «специалисты» все сделают сами. Сотрудник сразу же сообщает свой пароль, да еще и благодарит звонившего за помощь.

Как это выглядит на практике: после соответствующего согласования с руководством компании наши эксперты, представившись специалистами технической поддержки, позвонили сотруднику, ранее ответившему на фишинговое письмо. Под их диктовку пользователь зашел на поддельный корпоративный портал (было зарегистрировано доменное имя, содержащее дефис), а после того, как у него несколько раз не получилось ввести пароль, состоялся следующий диалог:

[Эксперт РТ]: Давайте вы просто свой пароль скажете, мы все на портале сделаем сами.

[Сотрудник]: О, так даже лучше. Мой пароль 978654321#!

[Эксперт РТ]: Хорошо, спасибо.

[Сотрудник]: Вы только не меняйте мне его, он очень удобный!

В отдельных случаях сотрудники просили позвонившего назвать свои имя и фамилию, и наши специалисты называли свои настоящие имена. Наиболее бдительные сотрудники проверяли наличие такого работника в компании и, если не находили, обрывали разговор. Стоит отметить, что злоумышленник может легко узнать необходимые данные заранее, используя соцсети или другие источники, где сотрудники раскрывают свои должности и контактные данные. Вероятно, результативность атаки после такой подготовки будет значительно выше.

…или в «Фейсбуке» напиши

Злоумышленники не пренебрегают поиском сотрудников компаний в социальных сетях, и атака на профиль окажется достаточно эффективной. Например, можно заразить вредоносным ПО устройство сотрудника, с которого он впоследствии подключается к внутренней сети компании или проверяет корпоративную почту. Недостаточно осведомленные в вопросах ИБ пользователи обсуждают в социальных сетях рабочие вопросы, обмениваются конфиденциальными документами, которые представляют высокую ценность для нарушителя. В отдельных случаях сотрудники могут использовать одинаковые пароли для доступа к социальной и

Заключение

Злоумышленники всегда будут использовать фишинг как для атаки на рядовых пользователей, так и с целью проникновения в корпоративную инфраструктуру. Причиной тому являются относительная дешевизна и простота таких методов, а также высокая эффективность.

Для рядовых пользователей самый актуальный и действенный совет – всегда оставаться бдительными, проверять информацию об отправителе, прежде чем перейти по ссылке или скачать предлагаемый файл, убедиться, что это не вредоносный ресурс. Полученные файлы перед открытием необходимо проверить с помощью антивирусного ПО, а если у компании есть специальная «песочница», то отправить файл в нее. Стоит также удостовериться, что домен легитимный и реальный. В случае сомнений рекомендуется проверить, действительно ли адресат отправлял данное письмо и является ли он настоящим владельцем домена и (или) электронного ящика, связавшись с ним каким-то альтернативным способом, например через мессенджер или по телефону. Если бы такую простую рекомендацию выполнили сотрудники при атаке со стороны группировки Cobalt, то это могло бы уберечь банки от многомиллионных потерь.

Что касается советов для IT- и ИБ-специалистов, то существует несколько простых технологий, повышающих защищенность от фишинговых атак по электронной почте. Например, настроенная SPF-запись защищает письма от подделки при отправке от имени вашего домена. Данная технология позволяет проверить подлинность сервера отправителя. Ее полезно использовать в сочетании с технологиями DKIM и DMARC. Первая дает возможность настроить соответствующую подпись, которая подтверждает, что адрес, указанный в поле «От кого», действительный, а вторая снижает количество фишинговых писем на основе правил и признаков идентификации почтовых доменов отправителя, заданных на сервере получателя. В качестве дополнительной меры защиты необходимо проверять PTR-запись для определения имени узла-адресата по его IP-адресу, а также наличие IP-адреса отправителя в спам-базах.

корпоративной сети либо незначительно изменять пароль, добавляя отдельные символы. Все полученные данные злоумышленник применит в свою пользу при развитии атаки на инфраструктуру.

Сегодня так действуют многие киберпреступники, например группировка SongXY, которая в 2017 г. принимала участие в атаках на промышленную отрасль и государственные учреждения стран СНГ. Злоумышленники искали профили сотрудников в социальных сетях и отправляли им сообщения. Кроме того, опасность заключается еще и в том, что сотрудники часто подключаются к социальным сетям с рабочих компьютеров, и тогда переход по ссылке, полученной от злоумышленника, может привести к прямому доступу к ЛВС организации. Более 70 % сотрудников охотно вступали в переписку, а 21 % перешли по предлагаемой ссылке. При целевой атаке злоумышленники будут использовать все доступные средства – социальные сети, мессенджеры. Поэтому, если в профиле социальной сети сотрудник указал свое место работы, он должен понимать свою ответственность за обеспечение ИБ и в нерабочее время.

Рекомендуется заблокировать доставку вложений по почте с расширениями, которые используются для исполняемых (.exe, .src), системных (.dll, .sys), скриптовых (.bat, .js, .vbs) и других файлов (.js, .mht, .cmd). Файлы с такими расширениями могут содержать вредоносный код, используемый злоумышленником при фишинговой рассылке. С более детальным перечнем таких расширений можно ознакомиться в соответствующих исследованиях[4].

Рекомендуется внедрить в инфраструктуру систему выявления вредоносного ПО, в которую сотрудники могли бы в любой момент загрузить на проверку почтовое вложение или любой другой файл. Специализированное антивирусное ПО позволяет выявлять вредоносные ссылки и файлы в корпоративной электронной почте до момента их открытия. Стоит отметить, что если злоумышленники используют обфускацию[5], то антивирусы могут не выявить вредоносное ПО сразу, поэтому стоит проводить анализ вложений не только перед открытием файла, но и ретроспективно. Это позволит как минимум выявить, что корпоративная система была скомпрометирована, определить дату компрометации и источник заражения, локализовать инцидент и провести более детальное расследование. Своевременное выявление и пресечение атаки позволит избежать серьезных последствий. Всегда остается актуальным совет своевременно устанавливать обновления ПО и ОС: это предотвратит эксплуатацию соответствующих уязвимостей.

Что касается организационных мер, то начинать надо с разработки и внедрения программы повышения осведомленности сотрудников в области ИБ. Хорошая практика, когда сотрудники оповещают своих «безопасников» о том, что им пришло фишинговое письмо, особенно если заметно, что над рассылкой тщательно поработали. В таком случае, даже если заражение или утечка имели место, еще можно успеть оперативно отреагировать на атаку и принять контрмеры.

[4] blueteamer.blogspot.ru/2017/05/, support.office.com/en-us/article/Blocked-attachments-in-Outlook-434752e1-02d3-4e90-9124-8b81e49a8519.

[5] Обфускация – процесс приведения исполняемого кода программы к виду, сохраняющему ее функциональность, но затрудняющему анализ, понимание алгоритмов работы и модификацию при декомпиляции.